AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

LODGED

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. JUSTIN ROBERTSON, Defendant.	DOCKET NO. ED 17-0276M
2017 JUN 14 PM 1:3 CLERK U.S. DISTRICT COURT CENTRAL DIST. OF CALIF. RIVERSIDE BY	MAGISTRATE'S CASE NO. 17-

FILED
CLERK, U.S. DISTRICT COURT
JUN 14 2017
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

Complaint for violation of Title 18, United States Code, Sections 1708

NAME OF MAGISTRATE JUDGE		LOCATION
HONORABLE SHERI PYM	UNITED STATES MAGISTRATE JUDGE	Riverside, California

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (IF KNOWN)
~~June 12~~, 2017 BB May 4,	Riverside County	

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

[18 U.S.C. § 1708]

On or about May ~~3~~ 4 BB, 2017, in Riverside County, within the Central District of California, defendant JUSTIN ROBERTSON ("ROBERTSON") unlawfully had in his possession mail which had been stolen from the mail, addressed to and from persons other than defendant ROBERTSON, knowing the same to have been stolen.

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT **Brad Barnes** /s/ OFFICIAL TITLE U.S. Postal Inspector – U.S. Postal Inspection Service

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE[1]	DATE
SHERI PYM	June 14, 2017

[1] See Federal Rules of Criminal Procedure 3 and 54

SAUSA Rebecca B. Shults x3144 REC: Detention

AFFIDAVIT

I, Brad Barnes, being duly sworn, declare and state as follows:

I. PURPOSE OF THIS AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrant for Justin Robertson ("ROBERTSON") for a violation of Title 18, United States Code Section 1708 (Possession of Stolen Mail).

2. This affidavit is also made in support of an application for a warrant to search the digital devices described in Attachment A ("ROBERTSON'S DEVICES"), which isincorporated by reference herein.

3. The requested search warrant seeks authorization to seize any data on ROBERTSON'S DEVICES that constitutes evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1704 (Possession of Counterfeit United States Postal Service Arrow Key), 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft), as more fully described in Attachment B, which is incorporated herein.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel,

specifically the Riverside County Sheriff's Department ("RCSD"). This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR POSTAL INSPECTOR BRAD BARNES

5. I am a United States Postal Inspector ("Postal Inspector") employed by the Los Angeles Division of the United States Postal Inspection Service ("USPIS"), San Bernardino Domicile, External Crimes Team. I have been so employed since July 2013. My responsibilities include the investigation of crimes against the United States Postal Service ("USPS") and crimes related to the misuse and attack of the mail system and assaults and threats against USPS employees, including: theft of United States mail ("U.S. Mail"); possession of stolen United States mail; crimes related to the use, theft, and counterfeiting of postal keys (referred to as "arrow keys") and locks; access device fraud; and identity theft. Additionally, I have received both formal and informal training from the USPIS regarding mail and identity theft.

6. Through my training and experience, I have learned that USPS delivers U.S. Mail to residents in neighborhoods via individual and community mail boxes. The USPS also provides blue collection boxes as a convenient way for USPS customers to

place outgoing mail for pickup by USPS employees. Mail thieves target individual boxes, community mail boxes, and blue collection boxes in effort to steal U.S. Mail. Mail thieves use crowbars, large screw drivers, and other tools to pry open the community mail boxes to access the mail. They also use homemade devices to steal from the blue collection boxes. The thieves refer to the method as "fishing." The homemade devices typically consist of a heavy device covered in a sticky substance on the end of a long string, strap, or belt. The heavy end is dropped into the collection box. The mail sticks to the heavy end and the thieves pull the string out and obtain the mail pieces. As a result of stealing mail, mail thieves can gain access to items such as checks, money orders, cash, and gift cards, as well as individuals' personal information, and use such information to commit bank fraud, check fraud, and access device fraud with credit cards and debit cards. Mail thieves conspire with other criminals, often called "connects", who assist in turning the information stolen from the mail into cash through bank fraud, check fraud, and access device fraud.

III. SUMMARY OF PROBABLE CAUSE

7. On May 3, 2017, during a traffic stop, Riverside County Sheriff's Department ("RCSD") Deputies found approximately 5 identification cards in other people's names, three access devices in other people's names, a magnetic card reader, a lamination machine, 56 checks in other people's names, and fishing tools. On May 4, 2017, during the execution of a state search warrant, deputies found hundreds of pieces of mail

in other people's names, a box of driver's licenses, license templates, and laminate sheets in ROBERTSON's bedroom.

IV. STATEMENT OF PROBABLE CAUSE

A. ROBERTSON'S INITIAL DETENTION

8. On May 26, 2017, I met with RCSD Deputy Brown regarding a case against ROBERTSON. Based on my discussions with Deputy Brown and my review of RCSD reports and evidence, I know the following:

a. On or about Wednesday, May 3, 2017, about 10:07 p.m. hours, RCSD Deputy Daniel Brown was on duty in Perris, California.

b. While on patrol, Deputy Brown saw a silver Nissan Altima with Oregon license plate number 577FWC, fail to stop at a stop sign. Deputy Brown initiated a traffic stop. Deputy Brown contacted the driver and explained the reason for the traffic stop. The driver, later identified as ROBERTSON, identified himself as J.N.R. and gave Deputy Brown a Nevada driver's license bearing the name J.N.R. Deputy Brown noticed the edges of the driver's license were frayed and the photograph appeared faded, which indicated to him that the identification card could be fraudulent.

c. ROBERTSON told Deputy Brown that he had been living at an address on El Nido Avenue in Perris for the past three months, and that he had not attempted to obtain a California driver's license.

d. Deputy Brown asked ROBERTSON to exit the Nissan to further investigate ROBERTSON's identity. Once ROBERTSON

exited the Nissan, Deputy Brown placed ROBERTSON under arrest for violation of California Vehicle Code section 12500(a), No Driver's License. Deputy Brown searched ROBERTSON's pockets incident to arrest and found the following:

i. A clear, zip-lock sandwich baggie containing a white crystalline substance located inside ROBERTSON's right front pants pocket. Deputy Brown recognized the substance as possibly being methamphetamine;

ii. A wallet found in ROBERTSON's pants pocket contained the following:

(I) A Washington state driver's license, displaying the name J.R.;

(II) Three California driver's license bearing the name B.D.;

(III) A military identification card bearing the name B.D.;

(IV) A second Nevada driver's license bearing the name J.N.R.

(V) A casino player's card in the name of J.N.R.;

(VI) A bank access cards displaying the name J.N.R.;

(VII) A bank access card with the name A.R. embossed on it; and

(VIII) A bank access card with ROBERTSON's name.

e. Deputy Brown walked ROBERTSON to his patrol car and explained that he was going to fingerprint ROBERTSON to ascertain ROBERTSON's true identity. ROBERTSON continued to insist that his name was J.N.R. Deputy Brown used an Integrated Biometric Identification System ("IBIS") to check ROBERTSON's thumbprints. The IBIS identified him as ROBERTSON.

f. Deputy Brown conducted a records check that showed that ROBERTSON had an active Riverside County felony warrant for forgery and fraud. ROBERTSON immediately said he wanted a lawyer present before speaking with Deputy Brown.

g. While Deputy Brown detained ROBERTSON, Deputy Adams spoke to the front passenger, Heather Mechelle Hutchinson ("Hutchinson"). Hutchinson told Deputy Adams the following:

i. Hutchinson and ROBERTSON just left ROBERTSON's residence on El Nido Avenue;

ii. The only property Hutchinson had inside the Nissan was her purse; and

iii. Hutchinson had a small amount of methamphetamine inside her purse. She gave Deputy Brown permission to remove it.

h. Deputy Provost found approximately 0.7 grams of methamphetamine and a glass methamphetamine pipe inside Heather's purse. Deputy Provost arrested Hutchinson for violation of California Health and Safety Code section 11377(a) possession of a controlled substance.

i. Deputy Provost and Deputy Brown conducted an inventory search of the Nissan, prior to the Nissan being towed. During the search, the deputies found the following:

i. A black backpack on the back seat containing:

(I) A MSRE206 magnetic credit card reader;

(II) 56 bank checks belonging to 26 different people; and

(III) A Scotch brand TL902 lamination machine; and

ii. A weighted piece of metal coated in an unknown sticky substance with a long string attached and wrapped in a cloth on the rear floorboard. Deputy Brown suspected that it was a "fishing tool" ROBERTSON used.

B. HUTCHINSON'S STATEMENTS

j. In a recorded, Mirandized statement, Hutchinson told Deputy Brown the following:

i. Hutchinson knows ROBERTSON as "Joel";

ii. Hutchinson and ROBERTSON have been dating for one month;

iii. Hutchinson spends several days each week at ROBERTSON's residence on El Nido Avenue;

iv. Hutchinson and ROBERTSON were at his residence prior to the traffic enforcement stop;

v. Hutchinson has seen templates for making fraudulent driver's licenses and identification cards inside ROBERTSON's bedroom;

vi. Hutchinson was unaware of anything illegal inside the Nissan; and

vii. Hutchinson never spoke with ROBERTSON about committing fraud.

C. INVESTIGATION OF ROBERTSON'S RESIDENCE

9. Based on my conversations with Deputy Brown and the evidence in this case, I know the following:

a. Deputy Brown took ROBERTSON to ROBERTSON'S residence on El Nido Avenue in Perris. Deputy Brown knocked on the front door and spoke with O.A. O.A. told Deputy Brown that she rented a bedroom in the house and confirmed that ROBERTSON also rented a bedroom in the house. Deputy Brown transported ROBERTSON to the RCSD Perris Station.

b. On or about May 4, 2017, RCSD deputies executed a state search warrant for ROBERTSON's residence. The deputies found the following in ROBERTSON's bedroom:

i. A piece of United States mail addressed to J.N.R. at ROBERTSON's residence, three altered bank access cards bearing J.N.R.'s name, and a piece of mail belonging to D.W. on a television stand;

ii. A black Epson color printer. Located in the back of the printer, deputies found the front of a California driver's license printed on a sheet of photo paper. The driver's license displayed the name E.S.B. and displayed a date

of birth and California driver's license number. Deputies confirmed that the printed driver's license number and date of birth corresponded to E.S.B.'s driver's license number and date of birth;

iii. Approximately 12 pieces of United States mail belonging to approximately twelve different people, including J.N.R., on a table in ROBERTSON's bedroom;

iv. A box of driver's licenses, driver's license templates, plastic card laminate sheets with magnetic strips, and the seal to the State of Nevada printed on a sheet of plastic. One of the Nevada driver's licenses displayed the name A.E.R, but displayed Hutchinson's picture. The driver's license had the counterfeit seal of Nevada printed on it;

v. Approximately 32 pieces of United States mail belonging to 17 different people and a glass pipe used to smoke methamphetamine in a cabinet;

vi. Approximately 28 pieces of United States mail belonging to 17 different people inside and atop a plastic storage container;

vii. A notebook containing the personal identifying information of 15 persons and a pack of Scotch brand thermal laminating pouches. The personal information contained first and last names, dates of birth, home addresses, social security numbers, credit card numbers and security codes for various people;

viii. An HP Envy 4511 copier/printer;

ix. A Sentry Safe[1] containing the following:

(I) Five Nevada driver's licenses each displaying ROBERTSON's photograph. The names and dates of birth on each of the five Nevada licenses were different. One of the names was C.J.B.;

(II) An Arizona driver's license and a Washington driver's license, both displaying the same photograph; and

(III) Two altered bank access cards;

x. A brown cardboard box containing a DMS-72A brand credit card embossing machine, two Scotch laminating machines, blank check stock, bank access cards, and a Cannon PIXMA photo printer;

xi. A Dell laptop Model number PP17L, P/N number NR139A00;

[1] Deputy Brown used the keys he found in ROBERTSON's pocket at the time of ROBERTSON's arrest to open the safe.

xii. An Apple computer with serial number C02MV4K1G085;

xiii. White Galaxy Express 3 smartphone, serial number R58HC4KJ23J;

xiv. ATT Tablet, model number K88 and FCC ID number SRQ-K88;

xv. A Tablet, model number EWT935DK and FCC ID number XHWEWT935DK;

xvi. A PNY 32 gigabyte ("GB") flash drive; and

xvii. A black Alcatel smartphone with IMEI number 35416107047551. (Collectively, "ROBERTSON'S DEVICES.")

D. MAIL THEFT VICTIMS

10. Based on my conversations with Deputy Brown, I know that:

a. Deputy Brown reviewed the evidence at the RCSD Perris Station. Deputy Brown found eight Wells Fargo bank checks bearing the names Jo.T and J.T. One of the checks, check number 9304, had the "Pay to the Order of" section cut off the check. Another check, check number 9288, was printed on regular paper and written to "M.M." for $150. Deputy Brown also found the original check number 9288 written to American Express Card. The back of the original check was signed M.M.

b. On or about May 4, 2017, Deputy Brown spoke with Jo.T via telephone. Jo.T. told Deputy Brown the following: On or about August 26, 2016, her mailbox was broken into and ten checks were stolen from within. She reported the incident to

the Riverside Police Department. Since the time of the theft, Jo.T. and her husband, J.T., have been the victims of identity theft. The suspect made over $2,100 in unauthorized purchases. Jo.T. does not know ROBERTSON and he did not have permission to be in possession of her bank checks.

c. On or about May 4, 2017, and May 5, 2017, Deputy Ortiz contacted seven additional victims whose mail or identification cards were found in ROBERTSON's house. All seven victims said that they did not know ROBERTSON or Hutchinson.

E. IDENTIFICATION CARD VICTIMS

11. Based on my conversations with Deputy Adams and Deputy Brown and my review of RCSD reports, I know that:

a. On or about May 4, 2017, Deputy Adams spoke with A.R. via telephone. A.R. told Deputy Adams that she did not know ROBERTSON or Hutchinson and neither of them had permission to be in possession of her personal information.

b. On or about May 5, 2017, Deputy Adams spoke with B.D. via telephone. B.D. told Deputy Adams that someone attempted to cash a $2,000 cashier's check using a forged California driver's license displaying B.D.'s name. B.D. told Deputy Adams that the person attempted to commit the fraud at the Bank of the West in Rancho Cucamonga on May 1, 2017.

c. On or about May 5, 2017, Deputy Brown contacted Bank of the West Corporate Security Investigator, Shannon Middleton, via telephone. Middleton gave Deputy Brown a photocopy of the forged driver's license that a man used to attempt to cash B.D.'s check at Bank of the West in Rancho

Cucamonga on May 1, 2017. The identification card was identical to the California driver's license ROBERTSON had in his pocket at the time of his arrest and an identification card found in ROBERTSON's bedroom. Middleton also gave Deputy Brown surveillance images taken from the transaction. Deputy Brown identified ROBERTSON from the images.

d. On or about May 5, 2017, Deputy Brown spoke to J.N.R. via telephone. J.N.R. told Deputy Brown the following:

i. J.N.R. currently lives in Las Vegas, Nevada;

ii. The address listed on the forged Nevada driver's license in ROBERTSON's possession is J.N.R.'s previous address;

iii. J.N.R. does not know ROBERTSON and did not give ROBERTSON permission to use his personal information to create forged driver's licenses;

iv. In December 2016, J.N.R. was contacted by Navy Federal Credit Union and alerted to suspicious activity on his account. The bank informed J.N.R. that a $1,300 check and a $2,300 check had been deposited into his account. J.N.R. did not make the deposits; and

v. J.N.R. recently noticed his credit score dropped significantly due to multiple credit inquiries.

e. On or about May 5, 2017, Hutchinson returned to the Perris Police Station. In a recorded, Mirandized statement, Hutchinson told Deputy Brown the following:

i. Hutchinson knew ROBERTSON made the forged Nevada driver's license with her photograph on it;

ii. ROBERTSON took the photograph from Hutchinson's Instagram account and altered it on his computer;

iii. ROBERTSON asked her to use the forged Nevada driver's license to commit fraud with him, and she refused;

iv. Hutchinson did not give ROBERTSON permission to make the forged Nevada driver's license;

v. Hutchinson never used the forged driver's license to commit fraud; and

vi. Hutchinson and ROBERTSON drove to a Bank of the West a few days prior to their arrests.

f. Following the interview, Deputy Brown placed HUTCHINSON under arrest for violation of California Penal Codes 470A (Forgery of a driver's license), 472 (counterfeit government seal), 484g (Fraudulent use of access cards), and 530.5(a) (identity theft).

V. TRAINING AND EXPERIENCE REGARDING MAIL THEFT AND BANK FRAUD

13. Based on my training and experience, including being a member of a USPIS Mail Theft Team, and information obtained from other law enforcement officers who investigate mail and identity theft, I know the following:

a. Mail thieves and/or members of mail theft rings steal mail in a variety of ways: breaking into panel mailboxes at apartment or condominium complexes, which allows the thieves access to numerous individual mailboxes at once; using stolen or counterfeit USPS arrow keys to open USPS collection or mailboxes; submitting fraudulent USPS "Change of Address" requests to divert mail from a victim's residence and forwarding

it to a suspect address or "drop" location; jamming USPS collection boxes with paper to allow someone to reach into the box; reaching into USPS collection boxes overflowing with U.S. Mail; "mailboxing," a process by which mail thieves drive through neighborhoods and steal outgoing and/or incoming U.S. Mail from residential mailboxes; and "fishing," which is using a homemade sticky device that is lowered into USPS collection boxes to extract U.S. mail through the deposit slot. Fishing devices typically have tape and/or glue on them, and mousetraps or flypaper are commonly used. Further, the mail drop door on USPS collection boxes limit the size of items and objects placed into them. Accordingly, mail thieves may also use inspection cameras with narrow flexible camera tubes to see inside USPS collection boxes to view the type and amount of mail in the box.

b. It is common practice for mail and identity thieves to keep "profiles" of victims, including on their digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, and driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

c. It is also common for mail and identity thieves to use digital devices to store information related to their identity theft crimes long after the crimes have been committed. This information can include logs of fraudulent transaction history; funds received; individuals and companies that have been victimized; payments from co-conspirators, and victim

profiles. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer id.

d. Based on my training and experience, I know individuals who participate in these schemes often work with co-conspirators to collect and use personal identifying and account information of their victims. These individuals often communicate by phone, e-mail, text message and social media, sometimes exchanging information and photographs related to their crimes.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

14. Based on my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives

intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

b. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

c. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory

or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

d. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes ("GB") of data are now commonplace. Consequently, each non-networked, computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

e. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an

active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

f. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image

as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

g. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone

else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

h. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

Instrumentality Protocol

15. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

16. Based on the foregoing facts, there is probable cause to believe that Justin ROBERTSON has committed a violation of Title 18, United States Code, Sections 1708 (Possession of Stolen Mail).

17. For the reasons described above, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses described in Attachment B will be found on the digital devices described in Attachment A.

/s/

Brad Barnes, Postal Inspector
United States Postal Inspection Service

Subscribed to and sworn before me this 14th day of June, 2017

SHERI PYM

UNITED STATES MAGISTRATE JUDGE